

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

1 1-48. (Cancelled)

1 49. (Currently amended) A method for managing a database system,
2 wherein the database system includes sensitive users, normal database
3 administrators, and security officers, comprising:
4 receiving a command to perform an administrative function involving a
5 user within the database system;
6 determining if the user is a sensitive user who is empowered to access
7 sensitive data in the database system;
8 if the user is not a sensitive user, and if the command is received from a
9 normal database administrator for the database system, allowing the
10 administrative function to proceed;
11 if the user is a sensitive user, and if the command is received from a
12 normal database administrator, preventing the normal database administrator from
13 performing the administrative function involving the sensitive user; and
14 if the user is a sensitive user, and if the command is received from a
15 security officer who is the only database administrator empowered to perform
16 administrative functions involving sensitive users, performing the administrative
17 function.

1 50. (Original) The method of claim 49, further comprising:
2 receiving a request to perform an operation on a data item in the database
3 system;

4 if the data item is a sensitive data item containing sensitive information
5 and if the request is received from a sensitive user who is empowered to access
6 sensitive data, allowing the operation to proceed if the sensitive user has access
7 rights to the sensitive data item; and

8 if the data item is a sensitive data item and the request is received from a
9 user who is not a sensitive user, disallowing the operation.

1 51. (Original) The method of claim 50, wherein if the data item is a
2 sensitive data item, if the operation is allowed to proceed, and if the operation
3 involves retrieval of the data item, the method further comprises decrypting the
4 data item using an encryption key after the data item is retrieved.

1 52. (Original) The method of claim 51, wherein the encryption key is
2 stored along with a table containing the data item.

1 53. (Original) The method of claim 52, wherein the encryption key is
2 stored in encrypted form.

1 54. (Original) The method of claim 49, wherein if the user is not a
2 sensitive user, and if the command to perform the administrative function is
3 received from a security officer, the method further comprises allowing the
4 security officer to perform the administrative function on the user.

1 55. (Currently amended) A computer-readable storage medium storing
2 instructions that when executed by a computer cause the computer to perform a
3 | method for managing a database system, wherein the database system includes

4 sensitive users, normal database administrators, and security officers, the method
5 comprising:

6 receiving a command to perform an administrative function involving a
7 user within the database system;

8 determining if the user is a sensitive user who is empowered to access
9 sensitive data in the database system;

10 if the user is not a sensitive user, and if the command is received from a
11 normal database administrator for the database system, allowing the
12 administrative function to proceed;

13 if the user is a sensitive user, and if the command is received from a
14 normal database administrator, preventing the normal database administrator from
15 performing the administrative function involving the sensitive user; and

16 if the user is a sensitive user, and if the command is received from a
17 security officer who is the only database administrator empowered to perform
18 administrative functions involving sensitive users, performing the administrative
19 function.

1 56. (Original) The computer-readable storage medium of claim 55,
2 wherein the method further comprises:

3 receiving a request to perform an operation on a data item in the database
4 system;

5 if the data item is a sensitive data item containing sensitive information
6 and if the request is received from a sensitive user who is empowered to access
7 sensitive data, allowing the operation to proceed if the sensitive user has access
8 rights to the sensitive data item; and

9 if the data item is a sensitive data item and the request is received from a
10 user who is not a sensitive user, disallowing the operation.

1 57. (Original) The computer-readable storage medium of claim 56,
2 wherein if the data item is a sensitive data item, if the operation is allowed to
3 proceed, and if the operation involves retrieval of the data item, the method
4 further comprises decrypting the data item using an encryption key after the data
5 item is retrieved.

1 58. (Original) The computer-readable storage medium of claim 57,
2 wherein the encryption key is stored along with a table containing the data item.

1 59. (Original) The computer-readable storage medium of claim 58,
2 wherein the encryption key is stored in encrypted form.

1 60. (Original) The computer-readable storage medium of claim 55,
2 wherein if the user is not a sensitive user, and if the command to perform the
3 administrative function is received from a security officer, the method further
4 comprises allowing the security officer to perform the administrative function on
5 the user.

1 61. (Currently amended) An apparatus that manages a database system,
2 wherein the database system includes sensitive users, normal database
3 administrators, and security officers, comprising:
4 a command-receiving mechanism configured to receive a command to
5 perform an administrative function involving a user within the database system;
6 an execution mechanism configured to,
7 determine if the user is a sensitive user who is empowered
8 to access sensitive data in the database system;

allow the administrative function to proceed, if the user is not a sensitive user, and if the command is received from a normal database administrator for the database system;

prevent a normal database administrator from performing the administrative function involving the sensitive user, if the user is a sensitive user, and if the command is received from the normal database administrator; and to

allow the administrative function to proceed, if the user is a sensitive user, and if the command is received from a security officer who is the only database administrator empowered to perform administrative functions involving sensitive users.

1 62. (Currently amended) The apparatus of claim 61,
2 wherein the command-receiving mechanism is configured to receive a
3 request to perform an operation on a data item in the database system;
4 wherein the execution mechanism is configured to,

allow the operation to proceed, if the data item is a sensitive data item containing sensitive information and if the request is received from a sensitive user who is empowered to access sensitive data, and if the sensitive user has access rights to the sensitive data item; and to

10 disallowing the operation, if the data item is a sensitive data
11 item, and the request is received from a user who is not a sensitive
12 user.

1 63. (Currently amended) The apparatus of claim 62, further
2 comprising a decryption mechanism, wherein if the data item is a sensitive data

3 item, if the operation is allowed to proceed, and if the operation involves retrieval
4 of the data item, the decryption mechanism is configured to decrypt the data item
5 using an encryption key after the data item is retrieved

1 64. (Currently amended) The apparatus of claim 63, wherein the
2 encryption key is stored along with a table containing the data item.

1 65. (Currently amended) The apparatus of claim 64, wherein the
2 encryption key is stored in encrypted form.

1 66. (Currently amended) The apparatus of claim 61, wherein if the user
2 is not a sensitive user, and if the command to perform the administrative function
3 is received from a security officer, the execution mechanism is configured to
4 allow the security officer to perform the administrative function on the user.